

REMARKS

In the Office Action¹, the Examiner objected to claims 4, 8, and 10, and rejected claims 1-5 and 7-10 under 35 U.S.C. 103(a) as being unpatentable over Cuervo et al. (Network Working group, RFC 3015, Megaco protocol Version 1.0 November 2000, "Cuervo") in view of Matsuzaki et al. (USPN 6058476, "Matsuzaki").

By this Amendment, Applicant has amended claims 1, 4, and 7-10. Reconsideration of the rejections and timely allowance of the pending claims 1-5 and 7-10 in light of the foregoing amendments and the following comments is respectfully requested.

Objection to Claims 4, 8, and 10

Claims 4, 8, and 10 have been amended to recite "said security data package," as suggested by the Examiner. Therefore, Applicant requests examiner to withdraw the objection to claims 4, 8, and 10.

Rejection of Claims 1-5 and 7-10 Under 35 U.S.C. §103(a)

Applicant respectfully traverses the rejection of claims 1-5 and 7-10 under 35 U.S.C. 103(a) as being unpatentable over *Cuervo* in view of *Matsuzaki*. A *prima facie* case of obviousness has not been established.

Independent claim 1 is patentable over *Cuervo* in view of *Matsuzaki* for at least the following reasons.

¹ The Office Action may contain a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

Claim 1 recites, in part, “configuring a Media Gateway (MG) with an authentication key and setting a security data package, which is a collection of a security authentication signal and an event, on a network protocol, by a Media Gateway Controller (MGC).” Applicant respectfully submits that *Cuervo* does not teach or suggest this element.

The examiner asserted that the session key in section 10.3 of *Cuervo* corresponds to the claimed “authentication key.” See Office Action, p. 3. Without acquiescing to this assertion, Applicant respectfully notes that the “session key” in *Cuervo* is “used to encrypt [] audio messages, protecting against eavesdropping.” *Cuervo*, section 10.3. Therefore, the session key of *Cuervo* is not used to configure the MG.

In addition, the examiner asserted that *Cuervo* teaches that “the MG’s plurality of security packets are set by MGC,” citing sections 7 and 10 of *Cuervo* for support. Office Action, p. 3. Section 7 of *Cuervo* describes various commands, such as Add, Move, and Modify. Section 10 of *Cuervo* covers security when using the protocol in an IP environment. However, Applicant respectfully notes that neither of the cited sections of *Cuervo* teaches a “security packet,” as alleged by the examiner. Nothing in *Cuervo* could constitute the claimed “security data package,” as recited in claim 1. Furthermore, *Cuervo* does not teach or suggest a “security data package” that “is a collection of a security authentication signal and an event,” as recited in claim 1.

In view of the above, *Cuervo* fails to disclose or suggest “configuring a Media Gateway (MG) with an authentication key and setting a security data package, which is a collection of a security authentication signal and an event, on a network protocol, by a Media Gateway Controller (MGC),” as recited in claim 1.

Moreover, claim 1 further recites, in part, “during a security authentication, sending by the MGC a security authentication request containing a security authentication parameter to the MG using the security data package” (emphases added). *Cuervo* also fails to disclose or suggest this element.

The Examiner asserted that the “ICV” in section 10.2 of *Cuervo* corresponds to the claimed “security authentication parameter.” See Office Action, p. 3. However, this assertion is not correct.

Specifically, in *Cuervo*, ICV (Integrity Check Value) is “calculated over the entire IP packet including the IP header . . . [to] prevent[] spoofing of the IP address.” *Cuervo*, section 10.2, (emphasis added). “To retain the same functionality, the ICV calculation should be performed across the entire transaction prepended by a synthesized IP header consisting of a 32 bit source IP address, a 32 bit destination address and a 16 bit UDP destination port encoded as 10 hex digits.” *Cuervo*, section 10.2, (emphasis added). In other words, the ICV in *Cuervo* is calculated by the information of the synthesized IP header to check the Integrity of the message so as to prevent spoofing of the IP address. *Cuervo* does not teach or suggest that the ICV is contained in a security authentication request sent by the MGC to the MG.

Therefore, *Cuervo* also fails to disclose or suggest “during a security authentication, sending by the MGC a security authentication request containing a security authentication parameter to the MG using the security data package,” as recited in claim 1.

Furthermore, the examiner asserted that section 10 of *Cuervo* discloses “determining by the MGC whether the MG is legal,” as recited in claim 1. See Office Action, p. 4. However, this assertion is not correct.

In *Cuervo*, a specific problem of packet is “uncontrolled barge-in.” See *Cuervo*, section 10.3. *Cuervo* teaches that “[t]his attack can be performed by directing media packets to the IP address and UDP port used by a connection.” *Cuervo*, section 10.3. “A basic protection against this attack is to only accept packets from known sources, checking for example that the IP source address and UDP source match the values announced in the Remote Descriptor.” *Cuervo*, section 10.3. In other words, the integrity check of *Cuervo* is to check the IP source address and UDP source in order to determine whether the packet is from known sources, and whether accept packets. There is no teach or suggestion in *Cuervo* to check whether the MG is legal.

Accordingly, *Cuervo* also fails to discloses “determining by the MGC whether the MG is legal” by comparing the calculation result obtained according to the security authentication parameter and the authentication key with a result calculated by the MGC,” as recited in claim 1

In view of the discussions presented above, *Cuervo* at least fails to disclose or suggest:

configuring a Media Gateway (MG) with an authentication key and setting a security data package, which is a collection of a security authentication signal and an event, on a network protocol, by a Media Gateway Controller (MGC);
during a security authentication, sending by the MGC a security authentication request containing a security authentication parameter to the MG using the security data package; [and]

...

determining by the MGC whether the MG is legal by comparing the calculation result obtained according to the security authentication parameter and the authentication key with a result calculated by the MGC.

Matsuzaki does not help bridge the gap between claim 1 and *Cuervo*. For at least the foregoing reasons, the combination of *Cuervo* and *Matsuzaki* does not disclose all the elements of claim 1. Thus, Applicant respectfully requests withdrawal of the rejection of independent claim 1, as well as dependent claims 2-5, as "dependent claims are nonobvious if the independent claims from which they depend are nonobvious." *In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992).

As claims 7 and 9 are independent claims reciting elements similar to claim 1, Applicant thus also respectfully requests withdrawal of the rejection of independent claims 7 and 9, as well as dependent claim 8 dependent from independent claim 7 and dependent claim 10 dependent from independent claim 9.

CONCLUSION

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,

GARRETT & DUNNER, L.L.P.

Dated: September 27, 2010

By: /Weiguo Chen/
Weiguo Chen
Reg. No. 61,878
(650) 849-6729